Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for Law Enforcement Act and Broadband Access and Services	)	ET Docket No. 04-295
	)	
	)	

COMMENTS OF GLOBAL CROSSING NORTH AMERICA, INC.

Global Crossing North America Inc., on behalf of its U.S. operating subsidiaries (collectively referred to as "Global Crossing"), hereby submits its Comments in support of the Petition for Reconsideration and Clarification of the First Report and Order and Further Notice of Proposed Rulemaking ("*Order*") submitted by the United States Telecom Association in the above-captioned proceeding.[1]

I. INTRODUCTION AND SUMMARY

Global Crossing provides telecommunications solutions over the world's first integrated global Internet Protocol- ("IP-") based network. Global Crossing is proud to have perhaps the most secure network in the telecommunications industry, having entered into a comprehensive network security agreement in September 2003 with the Departments of Justice, Homeland Security and Defense, and the Federal Bureau of Investigation. This precedent-setting agreement expressly obligates Global Crossing to provide technical or other assistance to Law Enforcement to facilitate electronic surveillance over its domestic facilities. The agreement not

---

[1] *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, RM-10865, FCC 05-153 (rel. Sep. 23, 2005) ("*Order*"); *Pleading Cycle Established For Petition For Reconsideration And Clarification Filed in the Communications Assistance For Law Enforcement Act And Broadband Access And Services Proceeding*, Public Notice, ET Docket No. 04-295, DA 06-7 (rel. Jan. 4, 2006).

only sets the bar higher for network security, but it enhances the company's long-standing culture of security.

In its *Order*, the Commission recognized that it had not yet addressed critical issues raised in its *Notice of Proposed Rulemaking*,[2] including "questions regarding the ability of broadband Internet access providers and [Voice over Internet Protocol ("VoIP")] providers to provide all of the capabilities that are required under section 103 of [the Communications Assistance for Law Enforcement Act ("CALEA")], including what those capability requirements mean in a broadband environment."[3] The Commission also has not yet addressed "a variety of issues relating to identification of future services and entities subject to CALEA, compliance extensions, cost recovery, and enforcement."[4] The Commission stated that it "will address each of these matters in a future order,"[5] which it has yet to issue. Despite the Commission's recognition that there is a complete lack of clarity as to what CALEA compliance means when applied to broadband Internet access and VoIP services, the Commission nevertheless has set an 18-month deadline from the effective date of the *Order* for providers of these services to reach "full compliance."[6] Pursuant to the *Order*, service providers must comply with CALEA or potentially face enforcement liability by May 14, 2007.

Global Crossing urges the Commission to grant the Petition and reconsider its May 14, 2007 compliance deadline in light of the *Order's* failure to provide any implementation

---

2 *Communications Assistance for Law Enforcement Act and Broadband Access Services*, Notice of Proposed Rulemaking, ET Docket No. 04-295, RM-10865, FCC 04-187 (rel. Aug. 9, 2004).

3 *Order* at ¶ 24.

4 *Id.*

5 *Id.*

6 *Id.*

guidelines for compliance as they relate to broadband Internet access and VoIP services. First, as is detailed below, the *Order* is arbitrary and capricious in that the record evidence on which the Commission relies simply fails to support the May 14, 2007 deadline provided in the *Order*. Second, the public interest is disserved by setting a deadline that is far shorter than any service provider indicated could be feasible. Especially for IP-based service providers with relatively small customer bases, such as Global Crossing, "full compliance" is not yet technically or economically feasible.

Therefore, the Commission should reconsider its decision to set a deadline of May 14, 2007 for CALEA compliance for broadband access and VoIP services providers, and instead begin the clock for compliance only after the Commission issues a further order setting forth the specific capabilities applicable to such services and "what those capabilities mean in a broadband environment."[7]

II. THE RECORD DOES NOT SUPPORT SETTING AN 18-MONTH DEADLINE FROM THE EFFECTIVE DATE OF THE *ORDER*

The Commission cites two rationales for setting an 18-month deadline, each of which are flawed and demonstrate a lack of reasoned decision-making. The Commission's first rationale for setting an 18-month compliance deadline is that this amount of time appeared reasonable based on suggested timeframes for compliance provided in the record.[8] The Commission cites a range of suggested deadlines to support its position, from the Department of Justice's suggested 12-month deadline to carriers suggesting a 24-month deadline.

Unfortunately, the Commission has taken these proposed compliance deadlines out of context. No commenter could have anticipated that the Commission would engage in this

---

7 *Id.*

8 *Id.* ¶ 46 n.138.

bifurcated ordering process whereby it would set a deadline for compliance, but explicitly leave *all* questions related to implementation for a later order, as the Commission has done here. The only reasonable reading of the record is that commenters estimated the time it would take to comply, assuming that the Commission provided the implementation guidance anticipated in the *NPRM*. The Commission's citation to the record for setting an 18-month deadline thus is arbitrary and capricious under the circumstances.

The second stated rationale for setting the deadline is the Commission's recognition that "nearly every commenter acknowledges the importance of assisting law enforcement agencies with their surveillance needs"[9] and that "many of these providers are already building CALEA capabilities into their networks and operations."[10] These good faith efforts should be seen as a reason to support a short delay in starting any mandatory compliance clock until the Commission provides further guidance. Instead, the Commission reasons that service providers' informal efforts toward compliance means that such service providers should be able to meet the 18-month deadline. There is a fundamental difference, however, between: (1) a provider doing its best to assist law enforcement, taking into account available technologies and the economic realities of particular services; and (2) a provider attempting to meet undefined statutory requirements that carry with them undefined enforcement liability for failure to comply. The Commission's approach is contrary to the Congressional mandate that there should be a balance between the needs of law enforcement and the needs of consumers and industry.[11]

---

9 *Id.* ¶ 47.

10 *Id.* ¶ 47 n.139.

11 House Report No. 103-827, 1994 U.S.C.C.A.N. 3489, 3493 ("[T]he bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly

CALEA is not intended to force service providers to deploy maximum surveillance capabilities. But that is the position in which the Commission's *Order* places broadband access and VoIP service providers. This is a completely different dynamic than the coordinated efforts between industry and law enforcement to which the Commission cites in its *Order*. The informal efforts of industry to assist law enforcement and build certain CALEA capabilities into their networks thus do not support the May 14, 2007 deadline.

III. THE COMMISSION'S 18-MONTH DEADLINE IS CONTRARY TO THE PUBLIC INTEREST

The Commission's decision to set a deadline for compliance far shorter than the industry requires disserves the public interest. As Motorola explained in its Comments in this docket, "Premature forced development of technical CALEA solutions will likely result in solutions that are unwise, inefficient, less effective, and perhaps soon obsolete."[12] Since well before the Commission issued its *Order* applying CALEA to broadband access and VoIP services, and continuing today, Global Crossing has been among the many IP-based services providers investigating ways to add CALEA capabilities to its IP-based network.[13] IP-based services, however, have their own unique technical issues, especially considering that consumers of broadband access services can engage service providers apart from the facilities-based provider, and can even self-provision services.

For example, to an IP-based network provider, such as Global Crossing, "bring-your-own" VoIP services often are indistinguishable from the constant deluge of other data packets traversing the network. Call identifying information often is buried under several layers

---

powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.").

12 Comments of Motorola, Inc., ET Docket No. 04-295, RM 10865, at 17 (filed Nov. 8, 2004).

13 Reply Comments of Global Crossing North America, Inc., ET Docket No. 04-295, RM 10865, at 6-9 (filed Dec. 21, 2004).

of data and is not "reasonably available" to the facilities-based broadband access services provider.[14] Thus, it often would not be reasonable to require the facilities-based carrier to be responsible for providing VoIP surveillance capabilities.

Moreover, IP-network providers cannot always isolate communications that are the target of a surveillance request. For example, an IP-network provider may only be able to provide *all* data traversing a particular business customer's network rather than communications to and from a particular surveillance target. This raises serious privacy concerns, and is directly analogous to situations that caused great concern to Congress, in which telecommunications carriers could not isolate communications coming through a PBX. As Congress observed:

> [T]here will be times when the telecommunications carrier will be unable to isolate the communications of a specific individual whose communications are coming through a PBX. This poses a minimization problem to which law enforcement agencies, courts, and carriers should be sensitive. The Committee does not intend the exclusion of PBXs to be read as approval for trunk line intercepts. Given the minimization requirement of current law, courts should scrutinize very carefully requests to intercept trunk lines and insist that agencies [explain] specifically how they will comply with the minimization requirement . . . . In addition, carriers presented with an order for interception of a trunk line have the option to seek modification of such an order.[15]

---

[14] *See, e.g.*, Comments of Level 3 Communications, LLC, Docket No. 04-295, RM 10865, at 12 (filed Nov. 8, 2004) ("In the ordinary course of Level 3's business, Level 3 is not aware of the third party applications or services that its customers may run, and it would require major modifications to Level 3's network to be able to detect, extract, and deliver third party-associated [call identifying information ("CII")] that may be in the packet stream. Such CII is typically in embedded layers of a packet not examined by Level 3's routers in the course of routing traffic to their destinations, and may be encoded using protocols completely unfamiliar to Level 3").

[15] House Report No. 103-827, 1994 U.S.C.C.A.N. at 3504.

For the same reasons, the Commission should be very cautious in imposing CALEA obligations on facilities-based broadband providers rather than the provider of the relevant individual service that is more likely to be able to isolate the information requested by law enforcement.

In addition to instances where CALEA capabilities are not technically feasible, the Commission must recognize that certain capabilities would come at such an economic expense as to make deployment "not reasonably achievable."[16] Especially for companies with small customer bases, compliance costs can be prohibitive. As GVNW observed in its Comments:

> While a large carrier may perhaps have the resources to accomplish this, it is absurd to believe that an ILEC or ISP with less than 50,000 customers has the resources to develop and deploy its own CALEA solution in the absence of one being available from its equipment vendors.[17]

Companies like Global Crossing, which provide specialized services to a relatively small customer base, do not have the resources or customer base of companies such as the Bell Operating Companies, and would be particularly harmed by the Commission's proposed transition schedule.

Similarly, a provider's right to cost recovery from law enforcement is crucial to the question of economic feasibility of implementation, especially in instances where extraordinary investment will yield minimal or no enhancements to national security and public safety. Indeed, institutions of higher education have noted that their costs of compliance could total billions of dollars.[18] Carriers such as Global Crossing that have been subject to no wiretap requests – and, because of the nature of their network and their customers, are unlikely ever to receive such a

---

16 *See* 47 U.S.C. § 1008(b) (setting out 11 factors for determining if compliance is not reasonably achievable, and, if such a determination is made, requiring law enforcement to pay for costs to make compliance reasonably achievable).

17 Comments of GVNW, ET Docket No. 04-295, RM 10865, at 5 (filed Nov. 8, 2004).

18 *See* Comments of The Higher Education Coalition, ET Docket No. 04-295, RM 10865, at 9, 10 (filed Nov. 14, 2005).

request – should not be required to make substantial capital expenditures for network upgrades. In such a case, the provider should be exempted from compliance or, in the alternative, law enforcement should be required to reimburse the provider for the costs of compliance.

IV. CONCLUSION

For the foregoing reasons, the Commission should grant the Petition for Reconsideration and set a reasonable compliance deadline only after the Commission issues further guidance on CALEA implementation in the context of broadband access and VoIP services.

Respectfully submitted,

GLOBAL CROSSING NORTH AMERICA, INC.

/S/

Teresa D. Baer
Jeffrey A. Marks
LATHAM & WATKINS LLP
555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004
(202) 637-2200

Its Counsel

Paul Kouroupas
Vice President, Regulatory Affairs
GLOBAL CROSSING NORTH AMERICA, INC.
200 Park Avenue, 3rd Floor
Florham Park, New Jersey 07932
(973) 937-0243

January 19, 2006

CERTIFICATE OF SERVICE

I hereby certify that I have this 19th day of January, 2006, caused a copy of the foregoing "Comments of Global Crossing North America, Inc." to be served by first class mail, postage prepaid, on the following:

James W. Olson
Indra Sehdev Chalk
Jeffrey S. Lanning
Robin E. Tuttle
United States Telecom Association
607 14th Street, N.W.
Suite 400
Washington, D.C. 20005

_/s/_____
Teresa D. Baer